



RECEIVED
JUN 14 2016

Joseph V. DeMarco
Telephone: 212.922.9499
jvd@devoredemarco.com

Computer Crime Section June 6, 2016

By First Class Mail

Computer Crime Section
Virginia Attorney General's Office
900 East Main Street
Richmond, VA 23219

Re: *Security Breach Notification*

Dear Sir or Madam,

We are counsel to Pasternack Tilker Ziegler Walsh Stanton & Romano, LLP ("Pasternack Tilker"). We write to inform you of a security breach which affected four Virginia residents whose personal information was stored on computer systems belonging to Pasternack Tilker. Please find attached a template of the letter we have sent to the affected Virginia residents, notifying them of the breach and offering them complementary identity theft protection services, which describes the circumstances of the incident.

Please feel free to contact us should you have any further questions regarding this matter.

Very truly yours,

Joseph V. DeMarco



99 Park Avenue, Suite 1100 New York, New York 10016 Telephone: 212.922.9499 Fax: 212.922.1799

www.devoredemarco.com

May __, 2016

[ADDRESS]

Re: Important Security and Protection Notification

Dear Sir or Madam:

I am writing to inform you that on July 9, 2014, Pasternack Tilker, LLP discovered that a now former employee of the law firm Napoli Bern Ripka Shkolnik, LLP ("Napoli Bern"), removed certain client data from a network system shared between our firm and Napoli Bern without authorization from either law firm. Pasternack Tilker has determined that a file containing your name, address, and/or Social Security number may have been included in the data that was removed. Due to a law enforcement hold that was in place while the authorities investigated this matter, we were unable to notify you of this breach of security at the time we learned of the incident. It is our understanding that the individual responsible for the incident has been apprehended and is currently facing criminal charges in Queens County, New York.

Pasternack Tilker takes the security of your personal information very seriously and we are truly sorry that this incident occurred. We are working with the law enforcement authorities to assist in investigating the incident and we are committed to ensuring that no similar incident occurs again. We are also committed to ongoing and comprehensive reviews of our data privacy and security protocols.

Identity Theft Protection Services

It is of paramount importance to us that you have confidence in our ability to safeguard your information. To help relieve your concerns and restore and maintain your confidence in us following this incident, we are offering you a **complimentary** one-year membership to Experian's® ProtectMyID® Elite. This product helps detect possible misuse of your personal information and provides you with platinum level identity protection support focused on immediate identification and resolution of identity theft.

Activate ProtectMyID Now in Three Easy Steps:

1. ENSURE That You Enroll By: **October 31, 2016**
2. VISIT the **ProtectMyID Web Site to enroll: www.protectmyid.com/enroll**
3. PROVIDE Your Activation Code: _____

If you have questions or need an alternative to enrolling online, please call 877-441-6943 and provide engagement #: _____.

Additional details regarding your 12-Month ProtectMyID membership:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
 - **Daily 3 Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax®, and TransUnion® credit reports.
 - **Internet Scan:** Alerts if your personal information is located on sites where compromised data is found, traded or sold.
 - **Change of Address:** Alerts of any changes in your mailing address.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
 - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **\$1 Million Identity Theft Insurance*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.
- **Lost Wallet Protection:** If you misplace or have your wallet stolen, an agent will help you cancel your credit, debit, and medical insurance cards.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-441-6943.

Assistance Hotline

If you have any questions or feel you have any identity theft issue call me at 516-471-1765, 8 a.m. to 5 p.m. (Eastern Time), Monday through Friday. I would be happy to answer your questions or help you with any concerns you may have.

Fraud Prevention Tips

We also wanted to make you aware of the incident and of the steps you should take to guard against identity fraud. We therefore recommend that you take the actions set forth in the **“Additional Recommended Steps to Protect Your Privacy”** (**ATTACHMENT A**) that we have included with this letter.

We take the protection of your personal information extremely seriously and will continue to take steps to ensure that a similar event does not happen in the future. We sincerely regret any inconvenience this incident may have caused you.

Sincerely,

Victor Pasternack

VP:zcl

ATTACHMENT A
Additional Recommended Steps to Protect Your Privacy

- **PLACE A 90-DAY FRAUD ALERT ON YOUR CREDIT FILE**

To protect yourself from the possibility of identity theft, we recommend that you immediately place a fraud alert on your credit files. An initial 90 day security alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. A fraud alert should not stop you from using your existing credit cards or other accounts, but it may slow down your ability to get new credit. You may contact any one of the credit reporting companies below for assistance, which will allow you to automatically place an alert with all of the agencies. You will receive letters from all three confirming the fraud alert and letting you know how to get a free copy of your credit report from each:

Equifax	800-525-6285	www.equifax.com
Experian	888-397-3742	www.experian.com
Trans Union	800-680-7289	www.transunion.com

- **PLACE A SECURITY FREEZE ON YOUR CREDIT FILE**

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. With a Security Freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting companies.

- **ORDER YOUR FREE ANNUAL CREDIT REPORTS**

Visit www.annualcreditreport.com or call 877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. In addition, please check for any medical bills that you do not recognize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

If you find suspicious activity on your credit report, or if you have reason to believe that your information is being misused, you may wish to file a police report of identity theft.

- **MANAGE YOUR PERSONAL INFORMATION**

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with and shredding receipts, statements, and other sensitive information.

- **USE TOOLS FROM CREDIT PROVIDERS**

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

- **OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF**

- Visit <http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html> for general information regarding protecting your identity.
- The Federal Trade Commission has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. You can also contact the FTC by mail at: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington D.C., 20580. They also provide information on-line at www.ftc.gov/idtheft.
- Contact the Virginia Attorney General by phone at 804-786-2071; or on the Web at <http://www.oag.state.va.us/citizen-resources/identity-theft>.